REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-18 are currently pending, Claim 1 having been amended to correct an informality. The changes and additions to the claims do not add new matter and are supported by the originally filed specification.

In the outstanding Office Action, Claims 1-18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lee (U.S. Pub. No. 2002/0080827) in view of Candelore (U.S. Pub No. 2005/0169473).

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. Claim 1 recites, *inter alia*,

> a packet determination part which determines from the received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal; and
>
> a cryptographic communication channel information agreement part which, if the packet determination part determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part.

Applicants respectfully submit that Lee and Candelore, taken alone or in proper combination, fail to disclose or suggest these features of amended Claim 1.

Lee is directed towards a buried data stream in a wireless home network. Figure 2 of Lee shows a gateway 100 that provides access to the Internet 10, external television and radio sources 12 to various appliances 180-188 in a house 20 (see para. [0045] of Lee). Gateway 100 includes a wireless transceiver 170 for transmitting data to appliances 180-188 (see para. [0057]). Gateway 100 also includes encryption/decryption unit 160 for encrypting data that

is transmitted wirelessly to the appliances 180-188 and for decrypting data received from appliances 180-188.

The Office Action acknowledges that Lee fails to disclose or suggest "a packet determination part which determines from the received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal; and a cryptographic communication channel information agreement part which, if the packet determination part determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part," as defined by Claim 1. (See Office Action, at pages 4-5).

The Office Action relies on Candelore to remedy these deficiencies of Lee with regard to Claim 1.

Candelore is directed towards a method of encrypting a digital television signal. Figure 2 of Candelore shows a set-top box (36 or 136) and Figure 6 shows a gateway set-top box (STB) 400. The set-top box decrypts encrypted content from a content provider and provides it for various appliances in a home network (see para. [0032]). Candelore describes that there can be different types of DRM systems, such as a CA system A or DRM system B, and the set-top box may be compliant with one of those systems (see para. [0054]-[0055]). Candelore describes that a set-top box compliant with system B receives a packet and determines if the packet is clear (unencrypted), encrypted under system A, or encrypted under system B. If the packet is clear it is passed directly to a decoder. If it is encrypted under system A (EA) then it is dropped. If it is encrypted under system B (EB) then it is decrypted. (See para. [0055]).

The Office Action takes the position that Candelore's description of a set-top box compliant with DRM system B discussed above corresponds to "a packet determination part which determines from the received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal." (See Office Action at page 7, citing Figure 5 and para. [0055] of Candelore).

However, as discussed above, paragraph [0055] of Candelore only describes determining whether the packet is clear, encrypted under CA system A or encrypted under DRM system B. In other words, Candelore describes determining whether a packet is unencrypted or encrypted by a specific system. At no point in this process does the set-top box determine "whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal." In other words, Candelore is just analyzing packets to determine if they should be bypassed, decrypted, or dropped, but this example does not describe that a determination on agreeing with a counterpart apparatus is ever made. On the contrary, in Candelore, no determination on agreement by the set-top box would even be necessary because the set-top box is already considered compliant with a particular system such as DRM system B.

Therefore, Applicants submit that Candelore fails to disclose or suggest "a packet determination part which determines from the received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal," as defined by Claim 1.

The Office Action also takes the position that Candelore describes a "cryptographic communication channel information agreement part which, if the packet determination part

determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part." (See Office Action at page 7, citing para. [0043] of Candelore). However, paragraph [0043] of Candelore only describes that the authorized set-top boxes receive Entitlement Control Messages (ECM) that are used to get access criteria and descrambling keys. The set-top box attempts to apply the key obtained from the ECM to the content. However, even if the access criteria or descrambling keys described by Candelore is considered "cryptographic communication channel information," there is no description in Candelore that the set-top box stores this access criteria or descrambling keys ***based on a packet determination part of the set-top box determining a necessity of agreement***. In other words, Candelore describes storing access criteria and descrambling keys in the set-top box, but never describes that the storing is made after the set-top box first determines that an agreement is necessary between the set-top box and a counterpart apparatus.

Therefore, Applicants submit that Candelore fails to disclose or suggest a "cryptographic communication channel information agreement part which, if the packet determination part determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part," as defined by Claim 1.

Therefore, Applicants submit that Candelore fails to remedy the deficiencies of Lee with regard to Claim 1. Thus, Applicants respectfully submit that Claim 1 (and all associated dependent claims) patentably distinguishes over Lee and Candelore, either alone or in proper combination.

Independent Claim 13 recites features similar to those of Claim 1 which were discussed above. Therefore, Applicants respectfully submit that Claim 13 (and all associated

dependent claims) patentably distinguishes over Lee and Candelore, either alone or in proper combination.

Applicants note that the above mentioned features of Claim 1 were addressed in Applicants' response to the previous Office Action, but the examiner did not specifically respond to those arguments. Additionally, Applicants submitted separate arguments with regard to dependent Claims 2, 3, 4, 8, 9-12, 16, and 17, but the examiner did not specifically respond to those arguments as well. Therefore, Applicants re-submit the arguments with respect to dependent Claims 2, 3, 4, 8, 9-12, 16, and 17 below.

With respect to the rejection of dependent Claim 2 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action takes the position that Lee describes the claimed filter information storage part on Figure 2 and paragraph [0051]. However, paragraph [0051] of Lee only describes that fire wall section 130 protects the house environment against undesired electronic intrusion through the WAN interface section 110. The fire wall section 130 of Lee does not determine whether or not to perform cryptographic processing. Therefore, Lee fails to disclose or suggest a filter information storage part which stores sending source identification information, sending destination identification information, protocol information indicating a packet communication procedure and ***processing instruction information indicating whether or not to perform cryptographic processing***, as filter information, as defined by Claim 2.

Additionally, because Lee fails to disclose the claimed filter information storage part, Lee also fails to disclose or suggest a cryptographic processing determination part which, ***by referring to said filter information storage part*** based on filter information in the packet received by the packet cryptographic processing apparatus, determines whether or not to perform cryptographic processing of the received packet by said cryptographic processing part based on the processing instruction information, as defined by Claim 2.

Candelore has been considered but fails to remedy the deficiencies of Lee with regards to Claim 2.

Thus, Applicants respectfully submit that Claim 2 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

Dependent Claim 14 recites features similar to Claim 2, therefore Applicants respectfully submit that Claim 14 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the reasons discussed above with regards to Claim 2.

With respect to the rejection of dependent Claim 3 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action relies on Candelore to remedy the deficiencies of Lee and disclose "a received packet determination part which determines whether or not a received packet from the counterpart apparatus which is forwarded to the terminal is valid." (See Office Action at page 5). Fig. 5 and paragraph [0055] of Candelore only describe determining whether the packet is clear, encrypted under CA system A or encrypted under DRM system B. However, Candelore fails to disclose or suggest a received packet determination part which determines whether or not a received packet from the counterpart apparatus which is forwarded to the terminal is valid, as defined by Claim 3.

Therefore, Candelore fails to remedy the deficiencies of Lee with regards to Claim 3.

Thus, Applicants respectfully submit that Claim 3 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

With respect to the rejection of dependent Claim 4 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action relies on Candelore to remedy the deficiencies of Lee and disclose that the use of a smart card in Candelore corresponds to the claimed "detachable, tamper-proof device in which at least part

of the cryptographic communication channel information is stored," as defined by Claim 4 (see pages 5-6 of the Office Action, citing para. [0022] of Candelore). However, Candelore does not disclose that the smart card includes a part of the cryptographic communication channel information, as defined by Claim 4.

Therefore, Candelore fails to remedy the deficiencies of Lee with regards to Claim 4.

Thus, Applicants respectfully submit that Claim 4 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

With respect to the rejection of dependent Claim 8 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action takes the position that Lee describes a terminal information collection part which collects the filter information and stores the information in said filter information storage part (see Office Action, at page 7, section 25, citing para. [0051] of Lee). Paragraph [0051] of Lee only describes that the fire wall section 130 protects the house environment against undesired electronic intrusion through the WAN interface section 110. However, Lee does not describe that the fire wall section 130 stores a part of at least one of the cryptographic communication channel information and the filter information, as defined by Claim 8.

Candelore has been considered but fails to remedy the deficiencies of Lee with regards to Claim 8.

Thus, Applicants respectfully submit that Claim 8 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

With respect to the rejection of dependent Claims 9-11 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action takes the position that Candelore remedies the deficiencies of Lee and describes a key information setting part, as defined in Claim 9 (see Office Action, at page 7, citing para. [0043] of Candelore). Paragraph [0043] of Candelore only describes that the set-top box attempts to

apply keys to the content. However, Candelore fails to disclose or suggest a key information setting part which sets key information for performing cryptographic processing of a packet, in the cryptographic communication channel information agreed by said cryptographic communication channel information agreement part, for the terminal, as defined by Claim 9.

Therefore, Candelore fails to remedy the deficiencies of Lee with regards to Claim 9.

Thus, Applicants respectfully submit that Claim 9 (and all associated dependent claims) patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

Dependent Claim 16 recites features similar to those of Claim 9. Thus, Applicants respectfully submit that Claim 16 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the reasons discussed above with regards to Claim 9.

With respect to the rejection of dependent Claim 12 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action takes the position that Lee describes a terminal information acquisition part, as defined in Claim 12 (see Office Action, at page 8, citing para. [0057] of Lee). Paragraph [0057] of Lee only describes a communication method of wireless transmitter 170. However, Lee fails to disclose or suggest a terminal information acquisition part which detects the terminal, acquires address information from the terminal and stores the acquired address information in said filter information storage part, as defined by Claim 12.

Candelore has been considered but fails to remedy the deficiencies of Lee with regards to Claim 12.

Thus, Applicants respectfully submit that Claim 12 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

With respect to the rejection of dependent Claim 17 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. The Office Action takes the position that Candelore remedies the deficiencies of Lee and describes performing the claimed determination about whether valid cryptographic communication channel information is stored in the cryptographic communication channel information storage part (see Office Action at page 10, citing Fig. 5 and para. [0055] of Candelore). Fig. 5 and paragraph [0055] of Candelore only describe determining whether a packet is clear, encrypted under CA system A or encrypted under DRM system B. However, Candelore fails to disclose or suggest that if the address information is stored, performing the determination about whether valid cryptographic communication channel information is stored in the cryptographic communication channel information storage part, as defined by Claim 17.

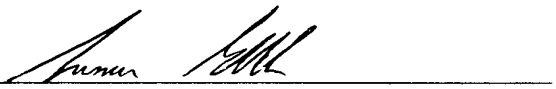
Therefore, Candelore fails to remedy the deficiencies of Lee with regards to Claim 17.

Thus, Applicants respectfully submit that Claim 17 patentably distinguishes over Lee and Candelore, either alone or in proper combination, for at least the foregoing reasons.

Consequently, in light of the above discussion, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Sameer Gokhale
Registration No. 62,618

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\SG\27's\277747US\277747US-AM2.DOC